IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:	Date: March 14, 2007
Bruce BENFIELD, et al.	Confirmation No: 5418
Serial No: 09/734,403	Group Art Unit: 2131
Filed: March 8, 2001	Examiner: Aravind K. Moorthy

Title: METHOD AND SYSTEM FOR INTEGRATING ENCRYPTION FUNCTIONALITY INTO A DATABASE SYSTEM

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P. O. Box 1450
Alexandria, VA 22313-1450

SUPPLEMENTAL BRIEF ON APPEAL

(1) Real Party in Interest

The real party in interest is International Business Machines Corporation by virtue of an assignment from the inventors recorded in the U.S. Patent Office on July 9, 2001, reel no. 011972, frame no. 0873.

(2) Related Appeals and Interferences

There are no appeals, interferences, or judicial proceedings known to Appellant, the Appellant's legal representative, or Assignee, which may be related to, directly affect, be directly affected by, or have a bearing on the decision by the Board of Patent Appeals and Interferences in the pending appeal.

(3) Status of Claims

Claims 1, 8, 15, 21-23, and 25-27 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,093,137 ("Sato").

Claims 2-4, 9-11, 16, and 17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sato in view of U.S. Patent No. 5,963,947 ("Ford").

Claims 6-7, 13-14, and 19-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Sato and Ford, in further view of U.S. Patent No. 6,360,322 ("Grawrock").

Claims 1, 8, 15, 21-23, and 25-27 are being appealed.

(4) Status of Amendments

There are no unentered amendments.

(5) Summary of Claimed Subject Matter

Of particular interest in today's computing environment are relational database applications. Relational DataBase Management System (RDBMS) software typically uses a Structured Query Language (SQL) interface. The SQL interface has evolved into a standard language for RDBMS software and has been adopted as such by both the American Nationals Standard Organization (ANSI) and the International Standards Organization (ISO). Specification, page 2, lines 1-6. The power of being able to gather, store, and relate information in database systems and then operate on that information through SQL allows for an almost limitless range of applications. Specification, page 2, lines 14-16.

However, there are concerns, particularly with regard to ensuring confidentiality of personal information, sensitive communications, and financial data. For example, users sometimes are required to input personal information, such as credit card information, for processing within a website. While security techniques may be used during the transmission of the data, within the database receiving and storing the information, the information remains accessible to the database administrator (DBA). Specification, page 2, lines 18-23. Unfortunately, the accessibility of the confidential, personal information of a user creates an opportunity for intruders/malicious DBAs to misuse the information. Specification, page 3, lines 2-4. The present invention is directed to aspects for integrating encryption functionality into a database system. Specification, page 3, lines 10-11.

Accordingly, independent claim 1 recites a method for integrating encryption functionality into a database system. The method includes providing at least two functions to support data encryption in a database system. Specification, page 5, lines 5–14. The method further includes utilizing the at least two functions within structured query language statements. Specification, page 5, line 18 – page 6, line 8.

Independent claim 8 recites a system for integrating encryption functionality into a database system. The system includes at least one computer processing device. Specification, page 4, lines 16-22; FIG. 1. The system further includes a database management system installed on the at least one computer processing device, in which the database management system supports utilization of at least two functions for data encryption Specification, page 5, lines 1-7; FIG. 1. The at least two functions for data

encryption are invoked within structured query language statements. Specification, page 6, lines 4-8.

Independent claim 15 recites a computer readable medium containing program instructions for integrating encryption functionality into a database system. The computer readable medium contains program instructions for providing at least two functions to support data encryption in a database system. Specification, page 5, lines 5–14. The computer readable medium further contains program instructions for utilizing the at least two functions within structured query language statements. Specification, page 5, line 18 – page 6, line 8.

Independent claim 21 recites a method for integrating encryption functionality into a database system. The method includes defining a function to support encryption of data in a database system, in which the encryption of data is based on a user-specified password, and the function has a function name. Specification, page 5, lines 12-15; page 7, line 1. The method further includes utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password. Specification, page 5, lines 18-23; page 6, lines 3-9. The structured query language statement includes the function name and the user-specified password. Specification, page 7, line 1.

Independent claim 25 recites a computer readable medium containing program instructions for integrating encryption functionality into a database system. The computer readable medium contains program instructions for defining a function to support encryption of data in a database system, in which the encryption of data is based on a

user-specified password, and the function has a function name. Specification, page 5, lines 12-15; page 7, line 1. The computer readable medium further contains program instructions for utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password. Specification, page 5, lines 18-23; page 6, lines 3-9. The structured query language statement includes the function name and the user-specified password. Specification, page 7, line 1.

(6) Grounds of Rejection to be Reviewed on Appeal

Applicant requests review as to claims 1, 8, 15, 21-23, and 25-27 and their rejection under 35 U.S.C. § 102(e) as being anticipated by Sato.

(7) Argument

1. Claims 1, 8, 15, 21-23, and 25-27 are not properly rejected under 35 U.S.C. § 102(e) as being anticipated by Sato.

(A) Claims 1, 8, 15

Claim 1 recites a method for integrating encryption functionality into a database system. In particular, the method includes providing at least two functions to support data encryption in a database system, and utilizing the at least two functions within structured query language statements (emphasis added).

Such a method has a potential advantage of providing a straightforward and flexible technique to protect confidential data in a database in a manner that allows integration with well-established, non-proprietary SQL techniques. Specification page 8, lines 3-10.

Sato discloses a database management apparatus that have the functions of encrypting and managing database (see Abstract; col. 6, ll. 25-31). Referring to FIG. 1, the database management apparatus includes a program storage device 314 that stores *a program* for realizing encryption of a database (col. 8, ll. 34-37). Specifically, the program performs the method shown in FIG. 2 when encrypting data within a database (col. 8, ll. 34-35).

(A)(i) Sato fails to disclose utilizing a function to support data encryption in a database system *within a structured query language (SQL) statement.*

Sato fails to disclose utilizing a function to support data encryption in a database system within a structured query language (SQL) statement. While Sato generally discloses ***a program*** that can encrypt data within a database, Sato fails to disclose that the program utilizes structured query language (SQL) statements, nor is it inherent that Sato's program utilizes structured query language statements to encrypt data in a database. *See* MPEP 2163.07 - "To establish inherency, the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill. Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999).

Moreover, Sato fails in general to disclose utilizing SQL – or SQL statements – with respect to database management. Thus, Sato cannot disclose utilizing at least two functions (that support data encryption) within a structured query language statement.

Claim 1 is, therefore, allowable over Sato.

Independent claims 8 and 15 each incorporates limitations similar to those of claim 1 and are, therefore, improperly rejected under 35 U.S.C. § 102(e) for at least the same reasons.

(B) Claims 21-23 and 25-27

Claim 21 recites a method for integrating encryption functionality into a database system. In particular, the method includes defining a function to support encryption of data in a database system, in which the encryption of data is based on a user-specified password, and the function has a function name. The method further includes utilizing the function within a structured query language statement, in which the structured query language statement ***includes*** the function name and the user-specified password.

Even assuming Sato were to disclose using structured query language statements during the encryption of data in a database (which Applicant does not concede), Sato fails to disclose utilizing a function (to support data encryption) within a structured query language statement – or any other language statement – in which the structured query language statement includes the function name and the user-specified password.

The Examiner cites column 26, lines 4-14 of Sato (reproduced below) as disclosing this limitation:

> Flash memory 36 is used as a storage device for storing a database 41 shown in FIG. 25. As shown in FIG. 25, the database 41 comprises information (non-public information) common among the members and information (public information) specific to each member. The information (non-public information) common among the members includes a production number, the user ID of each member of the group, and encryption key data (private key P1, P2). The information (public information) specific to each member includes encryption key data (public key P3, P4), and a password. The password is used as a part of the public key. Sato, col. 26, ll. 4-14.

In the cited portion above, Sato generally discloses a database 41 that stores non-public information and public information. And while Sato discloses that the public information (stored in the database 41) includes a password, Sato clearly fails to disclose that the password is utilized within a structure query language statement.

Claim 21 is, therefore, allowable over Sato for these reasons in addition to those reasons discussed above in connection with claim 1.

Claims 22-23, and 25-27 each incorporates limitations similar to those of claim 21 and are, therefore, improperly rejected under 35 U.S.C. § 102(e) for at least the same reasons as set forth in connection with claim 21.

(C) <u>The Examiner has not established anticipation under 35 U.S.C. §102.</u>

Anticipation under 35 U.S.C. §102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention. *Electro Med. Sys. S.A. v. Cooper Life Sciences*, 34 F.3d 1048, 32 USPQ2d 1017, 1019 (Fed. Cir. 1994). The Examiner has failed to show that the elements discussed in Sections (1)(A)-(1)(B) above are disclosed in Sato. Thus, claims 1, 8, 15, 21, and 25 are improperly rejected under 35 U.S.C. §102(e) as being anticipated by Sato. Claims 22-23 depend from claim 21 and are improperly rejected for those reasons set forth with respect to claim 21. Claims 26-27 depend from claim 25, therefore, these claims are improperly rejected for at least the same reasons.

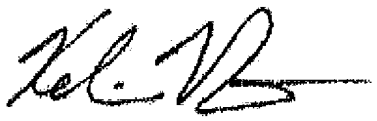
Conclusion

Sato fails to disclose utilizing at least two functions (that support data encryption) within a structured query language statement. Sato also fails to disclose utilizing a function (to support encryption of data) within a structured query language, in which the

structured query language statement includes the function name and the user-specified password. The Applicant, therefore, respectfully submits that claims 1, 8, 15, 21-23, and 25-27 are not properly rejected under § 102.

Please charge any fee that may be necessary for the continued pendency of this application to Deposit Account No. 09-0460 (IBM Corporation).

Respectfully submitted,
SAWYER LAW GROUP LLP



March 14, 2007
Date

Kelvin M. Vivian
Attorney for Applicant
Reg. No. 53,727
(650) 475-1448

Appendix of Claims

1. (Original) A method for integrating encryption functionality into a database system, the method comprising:

(a) providing at least two functions to support data encryption in a database system; and

(b) utilizing the at least two functions within structured query language statements.

2. (Original) The method of claim 1, wherein step (a) further comprises (a1) adding the at least two functions as user-defined functions in the database system.

3. (Previously Presented) The method of claim 2, wherein the user-defined functions further comprise a first function to encrypt user-specified data when inserted or updated in the database system.

4. (Original) The method of claim 3, wherein the user-defined functions further comprise a second function to decrypt the user-specified data when selected from the database system.

5. (Original) The method of claim 3, wherein the first function further encrypts the user-specified data with a user-specified password.

6. (Original) The method of claim 5, wherein the first function further encrypts with a password hint.

7. (Original) The method of claim 6, wherein the user-defined functions further comprise a third function to get the password hint.

8. (Previously Presented) A system for integrating encryption functionality into a database system, the system comprising:

at least one computer processing device; and

a database management system installed on the at least one computer processing device, the database management system supporting utilization of at least two functions for data encryption,

wherein the at least two functions for data encryption are invoked within structured query language statements.

9. (Original) The system of claim 8, wherein the at least two functions further comprise user-defined functions in the database management system.

10. (Previously Presented) The system of claim 9, wherein the user-defined functions further comprise a first function to encrypt user-specified data when inserted or updated in the database management system.

11. (Original) The method of claim 10, wherein the user-defined functions further comprise a second function to decrypt the user-specified data when selected from the database management system.

12. (Original) The system of claim 10, wherein the first function further encrypts the user-specified data with a user-specified password.

13. (Original) The system of claim 12, wherein the first function further encrypts with a password hint.

14. (Original) The system of claim 13, wherein the user-defined functions further comprise a third function to get the password hint.

15. (Original) A computer readable medium containing program instructions for integrating encryption functionality into a database system, the program instructions comprising:

(a) providing at least two functions to support data encryption in a database system; and

(b) utilizing the at least two functions within structured query language statements.

16. (Previously Presented) The computer readable medium of claim 15, wherein step (a) further comprises (a1) adding the at least two functions as user-defined functions in the database system.

17. (Previously Presented) The computer readable medium of claim 16, wherein the user-defined functions further comprise a first function to encrypt ~~the~~ user-specified data when inserted or updated in the database system, and a second function to decrypt the user-specified data when selected from the database system.

18. (Previously Presented) The computer readable medium of claim 17, wherein the first function further encrypts the user-specified data with a user-specified password.

19. (Previously Presented) The computer readable medium of claim 18, wherein the first function further encrypts with a password hint.

20. (Previously Presented) The computer readable medium of claim 19, wherein the user-defined functions further comprise a third function to get the password hint.

21. (Previously Presented) A method for integrating encryption functionality into a database system, the method comprising:

defining a function to support encryption of data in a database system, the encryption of data being based on a user-specified password, the function having a function name; and

utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password,

wherein the structured query language statement includes the function name and the user-specified password.

22. (Previously Presented) The method of claim 21, wherein the function is a user-defined function or a built-in function within the database system.

23. (Previously Presented) The method of claim 21, wherein defining a function to support encryption comprises:

defining an encrypt function to encrypt data when inserted or updated in the database system; and

defining a decrypt function to decrypt data when selected from the database system.

24. (Previously Presented) The method of claim 23, wherein:

the encrypt function further encrypts a password hint that assists a user in remembering the user-specified password; and

the method further includes defining a third function to get the password hint.

25. (Previously Presented) A computer readable medium containing program instructions for integrating encryption functionality into a database system, the program instructions comprising:

defining a function to support encryption of data in a database system, the encryption of data being based on a user-specified password, the function having a function name; and

utilizing the function within a structured query language statement to control access to the data in the database system including encrypting the data within the database system with the user-specified password,

wherein the structured query language statement includes the function name and the user-specified password.

26. (Previously Presented) The computer readable medium of claim 25, wherein the function is a user-defined function or a built-in function within the database system.

27. (Previously Presented) The computer readable medium of claim 25, wherein defining a function to support encryption comprises:

defining an encrypt function to encrypt data when inserted or updated in the database system; and

defining a decrypt function to decrypt data when selected from the database system.

28. (Previously Presented) The computer readable medium of claim 27, wherein:

the encrypt function further encrypts a password hint that assists a user in remembering the user-specified password; and

the method further includes defining a third function to get the password hint.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None